Hiding in Plain Sight: How Attackers Move Through the Network Undetected

Hacker Explains

Liam Cleary
Solution Architect
Protiviti

Jeff Melnick
Systems Engineer
Netwrix Corporation
Agenda

- Hiding
- Activities
- Preventing
Hiding
Hiding

Impersonation

Pivoting

Process Hijacking
Hiding: Impersonation

1. Retrieve Current User Tokens
2. Interrogate Environment for User Tokens
3. Impersonate Chosen User Token
4. Issue Commands as Impersonated User
5. Impersonate Chosen User Token
6. Retrieve Current User Tokens
7. Hacker
8. Client Workstation
Hiding: Pivoting

Server(s) → Client Workstation → Client Workstation Exploited → Hacker

- Requests sent from Client Workstation
- Commands returned to Hacker via Client Workstation
Hiding: Process Hijacking

Client Workstation

Interrogate Environment for Running Processes

Retrieve Current Running Processes

Inject into Selected Process

Issue Commands as Hijacked Process

Hacker
Activities
Activities

- Reconnaissance
- Scanning
- Access & Escalation
- Exfiltration
- Sustainment
- Assault
Activities: Reconnaissance / Scanning

Server(s) → Network Scanned for Servers → Client Workstation

Client Workstation → Send ARP Scan Request → Hacker

Hacker → Active Server(s) / Device(s) IP addresses Returned
Activities: Exfiltration

Folder(s) / Share(s) → SMB Share Request → Client Workstation → SMB Attack → SMB Share Accessed and Data Copied → Hacker
Preventing
Preventing

Whitelist Executables
Whitelist Scripts
Whitelist Locations

Blacklist Executables
Blacklist Scripts
Blacklist Locations
Preventing Client Workstation Execute Copied Filed Compromise Workstation Copy Executable Allowed Blocked Hacker App Locker Policy Checked
Demo
Takeaways
Takeaways

• Define App Locker policies to control executables, scripts and locations
• Inspect traffic on and off the servers
• Inspect traffic on and off workstations
• Utilize Firewall Isolation techniques on Windows Servers
Who: A visibility platform for user behavior analysis and risk mitigation = insider threats

What: Enables control over changes, configurations, and access
  • Focus on regulatory compliance
  • Investigate threat patterns before a data breach occurs

How: Provide security analytics
  • Detect anomalies in user behavior (who, what, when, where)
  • Provide actionable data
  • Reduce log event noise
Netwrix Auditor

Demonstration
Next Webinar

May 8th 11AM PT / 2PM ET

Privilege escalation: How hackers get elevated permissions → netwrix.com/webinars.html?webinar_id=435

Useful links

Free 20-Day Trial: setup in your own test environment
netwrix.com/data_discovery_and_classification.html#identify

Contact Sales to obtain more information: netwrix.com/contactsales
Thank you!

Liam Cleary
Solution Architect
Protiviti

Jeff Melnick
Systems Engineer
Netwrix Corporation

www.netwrix.com